State of Louisiana

DIVISION OF ADMINISTRATION
OFFICE OF THE COMMISSIONER

KATHLEEN BABINEAUX BLANCO
GOVERNOR

JERRY LUKE LEBLANC
COMMISSIONER OF ADMINISTRATION

DIVISION OF ADMINISTRATION

POLICY NO. 20

EFFECTIVE DATE: **May 20, 2003, Revised February 1, 2005**

SUBJECT: **Security of Information Technology Systems and Networks**

AUTHORIZATION: _____
Whitman J. Kling, Jr., Deputy Undersecretary

I. POLICY: Division of Administration (DOA) employees shall follow defined security practices in use of information technology systems and networks to protect the Division of Administration, its staff and resources. Information Technology Systems and Networks includes, but is not limited to, hardware, software, communications networks, physical facilities, mainframe computer, personal computers and printers, and personal hand held devices.

II. PURPOSE: To protect information technology systems and networks within the DOA.

III. APPLICABILITY: Applies to all employees within the DOA.

IV. PROCEDURE:

PASSWORDS
The proper use of a secured, confidential password is the easiest and most effective security tool available. Passwords should not be divulged to other persons and must be changed on a regular basis. The Office of Information Technology (OIT) has promulgated state standards for passwords in IT STD-009. The Office of Computing Services (OCS) guidelines for LAN passwords are documented in:

http://www.doa.state.la.us/ocs/security/password.htm

OCS shall periodically audit password use within the DOA for compliance to established standards.

VIRUSES
All computers connected to the DOA network including contractor desktops and laptops must have current anti-virus software installed and enabled. The virus definition updates and scans shall be scheduled to occur at least once a week.

WIRELESS DEVICES
Wireless networks have been proven to present security problems and require additional layers of protection to prevent unauthorized access. No wireless computer network system may be established or accessed within DOA buildings except those specifically authorized by the Office of Telecommunications Management (OTM).

MODEMS
Modem hardware attached to or installed in desktop computers systems connected to the network is prohibited. Laptop users are prohibited from using simultaneous connections via the modem and another network interface. Sections that require use of dial access to systems should contact OCS to identify alternatives.

LOCKDOWN
OIT Policy No. 005 defines the benefits and statewide guidelines for desktop power management and lockdown. To maximize security, facilitate support, and reduce costs, the DOA will disable administrative privileges on standard desktops. Based on business needs, a DOA section may request an exception be made for desktop power management and lockdown. The OIS contact can provide guidance in preparing the justification, which must state the business reasons for the lockdown exception request. Such requests for exceptions must be reviewed and approved jointly by the Office of Information Services (OIS) Director and the OCS Director.

The power management features shall be enabled on all desktop computers. Employees are expected to power off desktop computers and peripherals at the end of each work week.

SERVERS
No computer will be configured as any kind of server on the DOA networks without written approval from the OCS Director. Servers that will be accessed from more than one location must be housed within a data center environment.

V. RESPONSIBILITIES:

EMPLOYEE

The employee is responsible for adhering to the published IT security policy and taking reasonable steps to protect DOA computer systems and networks. If a virus is transmitted to a user's personal computer, the user is responsible for immediately

informing the OCS Help Desk. Each employee is also responsible for powering off desktop computers and peripherals at the end of each work week.

SECTION HEAD

Sections are responsible for documenting, on a case by case basis, the business reasons for any desired exception to the lockdown policy. Sections shall identify any application needs for dial-up usage and coordinate the use of modems with OCS in conformance with policy.

OFFICE OF TELECOMMUNICATIONS

OTM is responsible for the management and control of networks within the DOA. OTM will establish standards for wireless network use.

OFFICE OF INFORMATION SERVICES

The OIS Director is responsible for the review and approval of requested exceptions to the lockdown policy from a business perspective.

OFFICE OF COMPUTING SERVICES

The OCS Director is responsible for the review and approval of requested exceptions to the lockdown policy to ensure PC configuration changes associated with requested software will not interfere or jeopardize network security. OCS shall document and update the specific guidelines for password usage, incorporating OIT standards and industry practices. OCS shall check passwords periodically for adherence to rules, where possible. The OCS Director is responsible for approving any servers within the DOA.

DEPUTY UNDERSECRETARY

If joint approval of the OIS and OCS Directors can not be obtained for the requested exception to the lockdown policy, the Deputy Undersecretary will be responsible for granting the final approval/disapproval.